Yvon Avenel

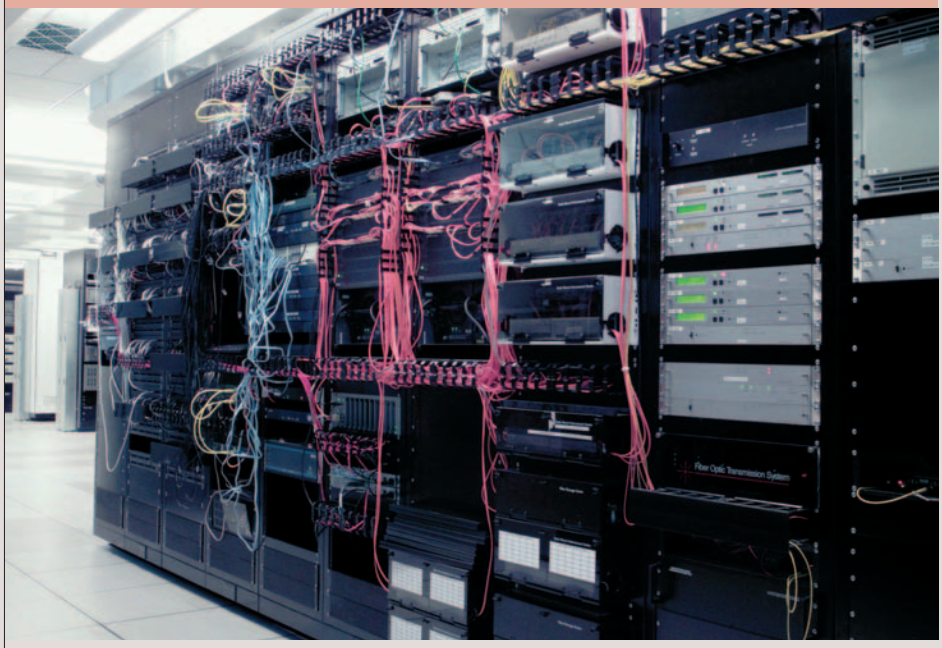
Journaliste
Éditeur de
SmartcardsTrends

SITES INFORMATIQUES

Les nouveaux outils de gestion et de maintenance

Tirés par la généralisation des réseaux IP, les outils de prise de contrôle à distance des sites informatiques – KVM en tête – apportent des solutions pour faire face à la montée des coûts de maintenance et répondre au besoin d'optimiser les temps d'exploitation.

OPTIMISER LES COÛTS DE MAINTENANCE



La complexité croissante des sites informatiques est due à l'acccroissement du nombre de serveurs et à celui de de leur densité.

L'activité des entreprises dépend, de plus en plus, de leur système d'information, et celui-ci, bien sûr, de ses propres infrastructures de production et de communication : postes de travail, grands systèmes, serveurs dédiés, routeurs, commutateurs, pare-feu, passerelles et réseaux divers, centres de données, de sauvegarde, salles blanches, systèmes d'alimentation électrique et de climatisation, etc. Ce constat de plus en plus trivial dans le secteur de la banque se double d'un autre qui mesure son aspect critique : 90 % des budgets informatiques [1] sont consacrés à des opérations de maintenance ; le coût d'un arrêt "système" serait de 14 millions de dollars par minute [2] pour une institution financière, sans commune mesure avec celui d'une usine moyenne qui, aux États-Unis, se chiffre entre 10 et 12 millions de dollars, mais par jour ! On comprend, dès lors, pourquoi l'objectif d'assurer une continuité de service, de prévenir les pannes, de réduire le MTTR (*Mean Time to Repair*) ou d'accroître le MTBE (*Mean Time Between Errors*), ou encore celui d'optimiser les temps d'exploitation, figure parmi les priorités des administrateurs de réseaux ou des DSI.

Mais ce souci devient, au fil du temps, aussi un défi. L'accroissement du nombre de serveurs [3], de leur densité (châssis embarquant de plus en plus de fonctions et multiplication de serveurs "lames"), de la complexité croissante qui en résulte, à quoi s'ajoute la montée en puissance des questions de sécurité, ont tendance à neutraliser les gains obtenus par ailleurs en matière de gestion pour réduire les pannes et améliorer les MTTR. IDC, dans une étude qui date de septembre 2004, souligne que les dépenses de gestion et d'administration des systèmes d'informations augmentent beaucoup plus vite (10 % par an) que celles consacrées à l'achat (sur la base de prix moyen très orienté à la baisse) de nouveaux serveurs (+3% par an). Et IDC de mettre le doigt sur les difficultés récurrentes à rendre productifs les moyens de gestion et d'administration dont les coûts continuent à croître dangereusement en pourcentage des coûts globaux de fonctionnement des sites informatiques. Enterprise Management Associates (EMA) confirme le diagnostic et pointe, dans son étude de juillet 2005, que la fragmentation très grande de l'offre en outils de gestion, de prise de

contrôle à distance, d'administration et de supervision pour surveiller, alerter, diagnostiquer, et réparer, est une source de coûts sans être pourtant la garantie d'une grande efficacité. Le bilan est donc sévère. "*95 % des outils de prise de contrôle à distance ou d'administration ne sont pas ou peu utilisés, 5 % seulement le sont à plein-temps*", souligne le directeur général d'une société spécialisée dans la fourniture de solutions de gestion de sites distants. En outre, certains outils réputés complémentaires comme les logiciels de gestion technique et les logiciels d'administration et de supervision sont parfois en partie redondants.

S'AFFRANCHIR DES DISTANCES

Pourtant, dans le domaine des sources d'économie et de productivité, ces outils de gestion à distance ou de prise en main à distance ont vite été identifiés comme le moyen de réduire les coûts de fonctionnement et de maintenance, voire d'apporter de nouvelles réponses (sécurité logique) aux problèmes de sécurité physique des accès aux salles informatiques. "*Notre offre de solutions de gestion à distance est maintenant clairement orientée autour d'un mot d'ordre : ne plus rentrer dans les data centers*", indique Christophe Bouniol, le directeur général d'Avocent France, qui défend par ailleurs le concept de "bunker informatique". L'étude, déjà citée plus haut, indique le cas où des frais de main-d'œuvre ont pu être réduits de 92 % grâce à la mise en place de dispositifs de gestion à distance, tandis que la durée effective de résolution des problèmes déclarés, a pu de son côté, être réduite de 66 %.

> *« Les dépenses de gestion et d'administration des systèmes d'informations augmentent beaucoup plus vite que celles consacrées à l'achat (sur la base de prix moyen très orienté à la baisse) de nouveaux serveurs. »*

Ces outils de gestion à distance ont également été vus comme un moyen d'optimiser l'utilisation de l'espace des salles informatiques. On estime, en effet, à 3 millions d'euros de coût d'installation d'un site informatique de 200 m², ce qui donne une idée du coût de la place occupée par le moindre écran ou clavier dédié à la gestion ou à l'administration.

Mais tous ces outils n'ont pas tout à fait la même fonction. Les logiciels de prise de contrôle des machines à distance – du type pcAnywhere (Symantec) qui permet dans ses dernières versions d'accéder à un hôte distant depuis un PDA, ou PC Share (Raritan), qui offre des solutions de travail collaboratif (jusqu'à 5 utilisateurs intervenant alternativement) sur une machine hôte distante, ou encore l'utilisation de protocole comme RDP (*Remote Desktop Protocol*) de Microsoft – ne peuvent être mis en œuvre qu'avec certains environnements et qu'à la condition que les machines hôtes soient en état de marche, ce qui est une contre-définition des situations dans lesquelles les opérateurs ou les techniciens sont amenés à intervenir... puisque c'est toujours en cas de panne ! C'est également le cas des logiciels de supervision ou d'administration – du type OpenView (HP), Tivoli (IBM) ou UnicenterTNG de Computer Associates – qui sont, entre autres, chargés de détecter des anomalies, faire remonter des alarmes, ou d'analyser la nature des trafics via des agents logiciels embarqués dans les machines et les équipements du réseau. Tous ces outils logiciels travaillent *in-band*, c'est-à-dire en utilisant les ressources du réseau opérationnel et les systèmes d'exploitation des machines en place. Du coup, ils supposent toujours l'intervention sur les sites des équipes de techniciens chargés de réparer ou de remettre en route les serveurs défaillants. Ce qui n'est le cas des KVM et des consoles séries ou des plateformes logicielles de gestion centralisée : ces équipements travaillent *out-of-band* [4] (câble Ethernet, port RS232 ou liaison IP/RTC redondante) et peuvent intervenir directement au niveau du BIOS des machines, même si le système d'exploitation connaît des problèmes. Ils sont ainsi capables de rebooter une machine, de relancer un système d'exploitation sur une autre partition, et ce, quel que soit le type environnement ou de plateforme.

RÉDUIRE LES ACCÈS PHYSIQUES

D'abord installés dans les sites informatiques, les KVM ont été déportés ensuite à l'extérieur de ces derniers (jusqu'à 300 m dans le même bâtiment), puis bien au-delà.

LE KVM : UNE REDÉCOUVERTE

K pour *keyboard* (clavier), V pour *video*, et M pour *mouse* (souris), le KVM est un commutateur (une matrice dotée d'un certain nombre d'entrées associées à des utilisateurs et de sorties vers des équipements, serveurs ou autres) qui permet de mutualiser l'accès à ces équipements, des serveurs graphiques ou non graphiques, équipements de réseau, NAS ou SAN. On évite ainsi de multiplier les écrans, les claviers et les souris, et on gagne en souplesse avec la capacité de passer d'un serveur à une autre en une fraction de seconde. Ce qui est souvent nécessaire en cas de panne. À l'origine, installés dans les salles informatiques sous la forme de racks reliés à un écran, ces KVM ont ensuite été déportés au-delà en séparant le rack qui est resté dans la salle informatique et l'écran, le clavier et la souris qui ont été installés à l'ex-

UNE REDÉCOUVERTE DU KVM

Le KVM est un commutateur équipé de plusieurs entrées (utilisateurs) et plusieurs sorties (serveurs). Les versions analogiques sont encore les plus répandues mais le marché du KVM IP (numérique) est en pleine expansion.

térieur, pour des problèmes de place et de dissipation thermique. Ces KVM, dits analogiques, sont aujourd'hui utilisés pour accéder à des équipements dont ils sont distants au maximum de 300 mètres. Cette distance est la limite physique pour transporter sur des câbles Ethernet (catégorie 5) sans perte, les signaux vidéo (VGA), du clavier et de la souris (PS/2 ou USB). Certaines installations font appel à des liaisons en fibre optique qui permettent d'étendre cette distance à 10 km environ. Tous les grands constructeurs de KVM – en France, ils sont trois : Avocent, Raritan et Minicom Advanced Systems – proposent des équipements qui disposent d'algorithmes de compression vidéo pour optimiser la résolution d'affichage, et des capacités en nombre d'utilisateurs qui varient de 1 à 64. Raritan vient ainsi d'annoncer un KVM (Paragon II V4.1) qui offre une résolution d'écran réglable jusqu'à 1600 x 1200 pixels sur 213 mètres. Dans cette gamme de KVM analogiques, celui qui offre 64 accès à des utilisateurs, peut adresser jusqu'à 10 000 serveurs.

DU "DATA CENTER" À L'AGENCE

"Le KVM a longtemps été considéré comme la troisième roue du carrosse", rappelle l'un des responsables de Raritan France, *"il y a encore 5 ou 6 ans, les KVM ne comptaient en général que 2 ou 4 ports, et ils étaient utilisés dans les salles informatiques pour travailler à des distances de quelques mètres (9 mètres maximum à l'époque) des équipements auxquels ils permettaient d'accéder. Leurs possibilités restaient du coup assez réduites. Ce n'est plus le cas désormais."* C'est donc aujourd'hui à une véritable redécouverte du KVM que l'on assiste.

Dans la panoplie des outils de gestion informatique, les KVM occupent, en effet, désormais une place centrale, et ce, pour plusieurs raisons. La première tient à leurs fonctionnalités proactives en termes de maintenance qui les distinguent des simples outils logiciels de prise de contrôle à distance, ou des outils de supervision dispensant leurs messages SNMP de façon somme toute assez passive. La seconde tient, on l'a vu, aux évolutions technologiques (distances, nombre de ports, etc.) qu'elles ont suivies depuis les années 2000. La troisième tient à une évolution majeure, plus récente celle-là – elle date de deux ou trois ans –, qui est liée à l'émergence et à la généralisation des réseaux IP. En effet, avec cette ouverture à Internet et au web, une nouvelle génération de KVM est en train de s'imposer en s'affranchissant de la notion de distance, à laquelle les technologies analogiques restent physiquement dépendantes. Les KVM IP (IP KVM Switches chez Minicom, Gamme Dominion chez Raritan, et gamme DSR et DSI chez Avocent) peuvent offrir à des utilisateurs localisés à Paris ou Singapour, un accès à des serveurs d'un site informatique basé à Bruxelles. D'où la résolution élégante de questions de maintenance à distance et d'administration qui réclamaient auparavant la mobilisation d'équipes d'astreintes liées physiquement à leurs sites d'intervention. Et ce, avec des coûts élevés et de fortes contraintes pour assurer le niveau de service demandé. L'IP a aussi permis d'apporter des réponses là où il n'y avait pas de solution quand les compétences techniques locales pour intervenir faisaient défaut. Maintenant, la réduction des coûts d'intervention va de pair avec l'assurance d'une bonne continuité du service ou, en tout cas, d'une amélioration de cette dernière.

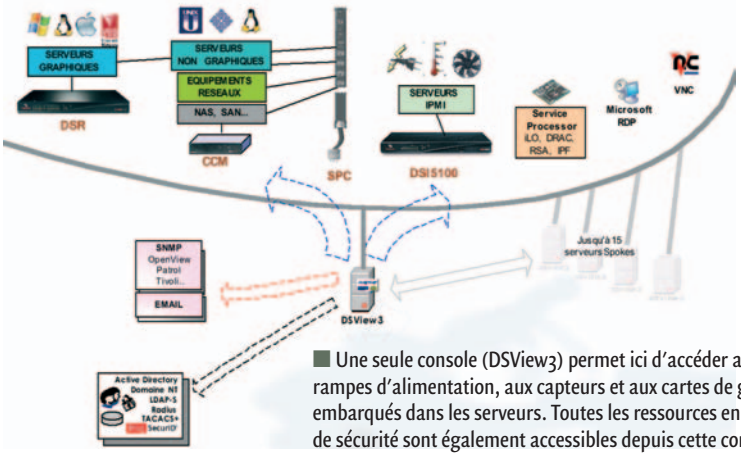
> *« Les KVM IP peuvent offrir à des utilisateurs localisés à Paris ou à Singapour, un accès à des serveurs d'un site informatique basé à Bruxelles. »*

Enfin, il y a sans doute une quatrième raison à l'intérêt renouvelé pour le concept de KVM. Elle s'exprime en particulier dans les agences bancaires et cette fois-ci concerne aussi les postes de travail : c'est la possibilité de déporter dans un local technique (*backracking*) les unités centrales des ordinateurs. Une façon de résoudre à la fois des problèmes de sécurité, et notamment celui posé par les risques encourus avec les utilisations malveillantes de clés USB [5], et celui de l'aménagement des bureaux (encore une fois le gain de place) dont l'ergonomie peut être améliorée en supprimant des sources de bruit et de chaleur. Dans ces cas, des KVM analogiques – encore beaucoup moins chers que les KVM IP – font parfaitement l'affaire. *"Il y a dans ce domaine pas mal de déploiements dans les banques aux États-Unis qui conjuguent la solution de problèmes techniques de maintenance et d'ergonomie des nouvelles agences"*, indique Christophe Bouniol, d'Avocent France, *"mais ici, en France, nous en sommes au stade des réflexions, dont certaines avancées, autour de concepts de locaux techniques organisés par région. On devrait voir des pilotes avant la fin de l'année."*

À LA RECHERCHE D'UNE APPROCHE GLOBALE

Les KVM IP n'ont pourtant pas la vocation de remplacer purement et simplement tous les KVM analogiques. Les trois grands constructeurs de KVM ont d'ailleurs à leur catalogue une offre de passerelles IP,

VERS DES SOLUTIONS GLOBALES



Une seule console (DSView3) permet ici d'accéder aux KVM, aux rampes d'alimentation, aux capteurs et aux cartes de gestion (IPMI) embarqués dans les serveurs. Toutes les ressources en matière de sécurité sont également accessibles depuis cette console.

capables de combiner les deux technologies. *"Nous avons développé des solutions comme Smart IP Access qui nous permettent de nous greffer sur l'existant, et de supporter même des commutateurs d'autres constructeurs"*, souligne un technicien chez Minicom. Chez Avocent, ce type de solution s'appelle SwitchView IP. IP joue un rôle fédérateur et unificateur. Sa généralisation a une autre conséquence : la virtualisation des accès et la possibilité de n'utiliser du côté "client" qu'un simple navigateur web pour accéder aux ressources d'un nombre illimité de serveurs et d'équipements, ont déjà favorisé le développement de solutions globales construites sur le concept de point d'entrée ou d'accès unique. Avocent propose ainsi une approche qui a l'ambition de centraliser à partir d'une seule console web (DSView3) la gestion informatique d'un ou de plusieurs centres de données en mutualisant les chemins d'accès à leurs serveurs et équipements, mais également à des outils complémentaires (outils SNMP, e-mail). Cette solution est en outre "sécurisée" grâce à la possibilité de la répliquer sur 15 serveurs différents. Elle permet de prendre tout aussi bien le contrôle d'une rampe d'alimentation, que de communiquer avec des capteurs de températures, d'humidité, que de prendre le contrôle de serveurs les plus divers, et notamment IPMI (*Intelligent Platform Management Interface Specification*), ou embarquant des cartes de gestion propriétaires (comme les cartes iLO de HP), enfin de s'interfacer avec des outils RDP (*Remote Desktop Protocol*) ou VNC (*Virtual Network Computer*). Chez Raritan et Minicom, les solutions de gestion centralisée (respectivement CommandCenter, et KVM.Net) sont davantage des consoles de pilotages du parc de KVM et de gestion de serveurs, même s'ils sont capables de gérer également via des adresses IP d'autres types d'équipements, comme les rampes d'alimentation.

MARIER SÉCURITÉ ET PERFORMANCES

Ces solutions IP qui "ouvrent", à partir d'un navigateur web, en quelque sorte, les portes des centres de données, doivent pourtant offrir le même niveau de sécurité que celui des systèmes de contrôles des accès physiques à ces mêmes centres. HTTPs et IP VPN sont donc utilisés d'emblée pour assurer les authentifications mutuelles des équipements entre lesquels s'ouvre une session ainsi que l'étanchéité des flux (*voir interview*). Les consoles de gestion sont ensuite toutes conçues pour gérer la sécurité des accès et administrer les droits de ces accès via des liens avec des ressources idoines comme des serveurs Radius, des annuaires et protocoles LDAP, TACACS, etc. Ils disposent également de capacités de chiffrement des données échangées entre les équipements et les KVM (RC4, 128 ou 256 bits SSL). Certains permettent l'utilisation de tokens (*challenge-response*, OTP) ou de cartes à puce (ou clés USB) pour assurer une authentification forte des opérateurs ou des administrateurs. Certains travaillent sur la possibilité d'utiliser des lecteurs biométriques pour remplacer les identifiants classiques. Tous ont développé des solutions qui conjuguent la sécurité et l'ergonomie. *"Plus c'est simple, plus c'est sûr : dès qu'un utilisateur s'authentifie, la liste des serveurs dont l'accès lui est autorisé apparaît à l'écran. Rien ne lui permet alors de sortir de ce cadre"*, explique Dennis Adda, le directeur commercial France de Minicom. La sécurité peut avoir un impact sur les performances, mais les constructeurs ont concentré leurs efforts sur l'optimisation de la bande passante grâce à la mise en œuvre d'algorithmes de compression vidéo. Il est, en effet, impératif de pouvoir ajuster la résolution à l'écran de façon à éviter des décalages entre les mouvements de la souris, et ceux de l'écran. ■

GLOSSAIRE

■ **Serveurs "lames" :** serveurs qui sont embarqués dans des châssis dont ils partagent les ressources (port Ethernet et connectique, processeur de supervision, alimentation, ventilateur). L'intérêt de ce type de configuration réside dans sa compacité et sa modularité.

■ **BIOS** (*Basic Input Output System*) : c'est un système de gestion élémentaire qui, au démarrage d'une machine (serveur ou poste de travail) établit et teste la configuration des composants (contrôleurs, mémoires), sous-systèmes (cartes, etc.) et ressources auxquels fait appel ensuite le système d'exploitation.

■ **SNMP** (*Simple Network Management Protocol*) : protocole qui permet aux administrateurs réseau de gérer et de diagnostiquer les problèmes survenants dans les équipements (commutateurs, routeurs, passerelles, etc.) via une console dédiée et des "agents" embarqués dans les équipements.

■ **"In-band"** (IB) ou **"out-of-band"** (OOB) : désignent la façon dont les outils de gestion informatique accèdent à distance aux machines ou aux équipements du réseau. "In-band" : par le réseau opérationnel utilisé précisément par ces machines. "Out-of-band" : via des liens spécialisés (Ethernet Cat 5, fibre optique, ou IP/RTC avec une redondance assurée par une liaison modem si le réseau IP est défaillant).

■ **IPMI** (*Intelligent Platform Management Interface Specification*) : une spécification qui décrit une interface commune et sécurisée pour surveiller des matériels et des capteurs (température, tension, ventilateurs, etc.), et contrôler des composants d'infrastructure (alimentations électriques, lames, etc.). Elle assure également la façon de consigner des événements système importants (intrusion dans le châssis, réinitialisation d'un système, etc.).

■ **LPAP** (*Lightweight Directory Access Protocol*) : protocole d'accès et de dialogue avec des services d'annuaires qui recensent des utilisateurs à qui sont attachés des attributs (noms, prénoms, organisation, adresses diverses, etc.) et des droits (attributs opérationnels).

NOTES

[1] Selon une étude récente de Celent Communications qui chiffre le coût de la maintenance informatique des banques européennes à quelque 41,3 milliards en 2005.
[2] Selon une étude réalisée en juillet 2005, par Enterprise Management Associates (EMA), pour le compte de la société Raritan.
[3] Selon une étude IDC (septembre 2004), le nombre de serveurs livrés dans le monde en 2003, était de 5,2 millions d'unités. Pour 2008, ce nombre pourrait pratiquement doubler (9 millions d'unités prévues). Quant aux serveurs "lames", ils étaient environ 185 000 à avoir été livrés pendant l'année 2003. Ils devraient représenter un marché de 3 millions d'unités en 2008.
[4] On dit également que ces équipements travaillent de façon non-intrusive. Rien n'est installé, ni logiciel ni matériel, sur les machines auxquelles ils accèdent.
[5] Ces clés faciles à installer sur une machine peuvent être utilisées pour le vol de fichiers.